	MILITARY HEALTH SYSTEM (MHS) **INFORMATION ASSURANCE (IA) IMPLEMENTATION GUIDE**	**IMPLEMENTATION GUIDE No. 3** **EFFECTIVE DATE** 07/19/05 **REVISED DATE** xx/xx/xx
Subject: **INCIDENT REPORTING AND RESPONSE PROGRAM**		

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

The term "MHS Information System (IS)" encompasses all automated IS applications, enclaves, outsourced IT-based processes, and platform information technology (IT) interconnections as defined in DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

This implementation guide emphasizes the importance of developing an Incident Reporting and Response Program and outlines the reporting procedures. All TMA Components should be aware of the security measures contained herein as a prompt and coordinated response can limit or prevent further damage, restore a system to operational status, and provide technical and administrative correction to protect the system from further attacks. Any event with the potential to adversely affect a MHS IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service is a threat and should be considered a computer security incident.

Computer security incidents are caused by policy and procedure violations, as well as outside intrusions and the exploitation of system vulnerabilities. These events could result in loss of data integrity, denial of system resources, penetration of a system's defenses either by an insider or an outsider, misuse of legitimate computer resources, or damage to information or resources.

An effective response to computer security incidents requires prompt recognition of the problem and immediate mobilization of a skilled staff. Prior documentation of procedures and clear delegation of responsibilities are necessary when responding to any computer security incident.

Essential components of a computer incident response are the elimination of points of vulnerability and the application of lessons learned.

1.1 The Federal Information Security Management Act (FISMA) mandates procedures for detecting, reporting, and responding to computer security incidents. A formal computer incident response capability minimizes the damage that can result from hackers, computer viruses, and other malicious code that threaten DoD ISs and networks.

1.2 The Health Insurance Portability and Accountability Act (HIPAA) Security Rule defines security incidents as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system." As outlined above, security incidents include, but are not limited to, policy violations by users, denial of service attacks, instructions, and unauthorized disclosures.

1.3 The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01D, "Information Assurance (IA) and Computer Network Defense," 15 June 2004, is the governing policy that describes how computer security incidents should be managed. The CJCSI 6510.01D provides detailed instruction on information security and outlines procedures for handling information technology security incidents within the DoD.

1.4 DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD IS and networks covered under DoD Directive (DoDD) 8500.1, "Information Assurance (IA)." DoDI 8500.2, Enclosure 4, provides IA Controls for vulnerability and incident management.

1.5 To maintain a proactive approach to vulnerability management, the MHS has implemented and manages the IA Vulnerability Management (IAVM) program for the TMA Components. MHS IA Implementation Guide No. 12, "The Information Assurance Vulnerability Management (IAVM) Program," provides further details to the MHS IAVM process.

2 POLICY

It is MHS Policy that:

2.1 TMA Components shall establish general procedures for responding to computer security incidents. Procedures should include guidelines on how the sites should:

a. Prepare a response to computer security incidents.

b. Analyze all available information to characterize a computer security incident including the determination of whether protected health information (PHI) was or was not involved.

c. Communicate with all parties that need to be made aware of a computer security incident and its progress.

d. Collect and protect information associated with a computer security incident.

e. Apply short-term solutions to contain a computer security incident.

f. Eliminate all means of vulnerability pertaining to a computer security incident.

g. Return information systems to normal operation.

h. Properly come to closure – identify and implement security lessons learned.

2.2 The Information Assurance Officer (IAO) shall develop written procedures, which comply with DoD and HIPAA Security Rule guidelines, to identify all actions needed to address and respond to a computer security incident.

2.3 The IAO and System Administrator (SA) shall establish a Computer Incident Response Policy and Computer Incident Response Team (CIRT). The IAO ensures that the CIRT conducts and documents an annual drill to practice the procedures of responding and handling computer incidents. The Computer Incident Response Policy shall include specific guidance on appropriate procedures for incidents involving PHI. The CIRT is encouraged to hold several drills annually and provide documented computer incident response training. Documented training should be maintained with the IA Training and Education files, which should be located with the site's training coordinator. The documentation should include as a minimum:

a. Who conducted the drills.

b. When drills were conducted.

c. Where drills were held.

d. What methodology was used.

2.4 The organization's IAO shall develop a Computer Security Incident Response Plan. At a minimum, the plan shall:

a. Identify the responsible Computer Network Defense Service Provider.

b. Define reportable computer security incidents.

c. Outline a standard operating procedure for incident response.

d. Notify the Chain of Command.

e. Identify communication procedures in the event a computer security incident becomes a media event, to include notifying General Counsel, Public Affairs, and local law enforcement agency.

f. Require periodic user training regarding the handling process of computer security incidents and reporting procedures.

g. Require the development of an incident handling checklist to provide the major steps to be performed.

h. Establish and train a CIRT comprised of at least the Information Assurance Manager (IAM), IAO, Network Managers, HIPAA Security Officer, and SA.

3 INCIDENT REPORTING

3.1 Computer security incident reporting is the notification provided to higher and/or lower echelons regarding out-of-the-ordinary events such as a loss of data integrity, a denial of system resources, the penetration of a system's defenses either by an insider or an outsider,

the misuse of legitimate computer resources, or the actual damage to information or resources.

3.2 A reportable incident/event is defined as, but not limited to:

a. Any intrusion into a network with a perceived unauthorized result.

b. Any loss or suspected loss of PHI or DoD sensitive information (SI).

c. Any unauthorized access or suspected unauthorized access to PHI or DoD SI.

d. A system alarm or similar indication from an intrusion detection tool.

e. Unexplained new user accounts.

f. Poor system performance.

g. "Door knob rattling" (e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts).

h. Unusual time of usage (note: more security incidents occur during non-working hours than any other time).

i. Any unauthorized privileged user, administrator, or root level access of a DoD System.

j. Any indications of Denial of Service or Distributed Denial of Service attacks.

k. Any new virus or worm for which no published countermeasure exists, any new virus whose propagation could likely outrun DoD containment capabilities, or any new virus that affects network services (e.g., e-mail and domain name system services).

l. Any root level access on a system using new methods that exploit significant vulnerabilities shared by DoD systems.

m. Any incident involving a Web server (e.g., www.army.mil, www.dtic.mil).

Although none of these events, taken singly are conclusive evidence of a security incident in progress, observing any of these should prompt an investigation. It is extremely important to obtain a full backup of the system in which suspicious events have been observed as soon as the possibility that a security-related incident has occurred or is indicated.

All TMA Components shall report incidents (or reportable events) affecting collateral networks directly to the DoD Computer Emergency Response Team (CERT) as indicated in the CJCSM 6510.01, "Defense-in-Depth, Information Assurance (IA) and Computer Network Defense (CND)," dated March 25, 2003.

4 PROCEDURES

4.1 The following computer security incident response procedures are provided as baseline requirements for an incident response plan. Each organization may determine their own specific procedures to satisfy communications and management requirements for handling and reporting a computer security incident:

a. Analyze the incident.

b. Contain or eradicate the problem.

c. Provide workarounds or fixes.

d. Prevent re-infection.

e. Log events.

f. Preserve evidence.

4.2 Once a computer security incident is detected, it should be reported to the appropriate IAO or Help Desk. All users shall know how to contact the IAO or the Help Desk to report suspicious events by telephone, in person, or via e-mail. If a user is reporting an incident affecting a computer or system, the user shall stop working on the affected computer or system, and the machine is to remain on.

4.3 The IAO is responsible for reporting the computer security incident information to the IAM. Additionally, the IAO should be prepared to advise the IAM on immediate response decisions in the event of a serious breach of security or the compromising of PHI or SI. If there is evidence of criminal activity, it is the IAO's responsibility, in concert with leadership, to notify the appropriate criminal investigative services.

4.4 If an incident occurs, the Director, Network Operations, and the IAM should take the following steps to notify the appropriate CIRT. The Director, Network Operations and the IAM shall make a determination to activate the local CIRT or to notify the Services' CIRT.

4.4.1 For computer incidents that occur with TRICARE contractors, the IAM/IAO shall comply with specific corporate incident response procedures. Additionally, TRICARE contractors are required to notify the Designated Approving Authority (DAA) via telephone immediately, follow-up with an e-mail, and complete the MHS Computer Security Incident Form (see Attachment 1), sending copies to the DAA and the MHS IA Program Office.

4.4.2 In all cases where DoD SI, PHI, or beneficiary information has been compromised or has had the potential of being compromised, Health Affairs (HA)/TMA leadership must be notified. HA/TMA notification should be made by Service Medical Department/Component senior leadership. For TRICARE contractors, the Chief Information Officer must notify HA/TMA.

5 REFERENCES

a. Federal Information Security Management Act of 2002 (FISMA)

b. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

c. DoDD 8500.1, "Information Assurance (IA)," October 24, 2002

d. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

e. DoDD O-8530.1, "Computer Network Defense (CND)," January 8, 2001

f. DoDI O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001

g. CJCSM 6510.01, "Defense-in-Depth, Information Assurance (IA) and Computer Network Defense (CND)," March 25, 2003

h. CJCSI 6510.01D, “Information Assurance (IA) and Computer Network Defense,” June 15, 2004

i. Standard Operating Procedures, “TMA Communications and Management of Unauthorized Electronic Information Disclosure Incidents”

6 ACRONYMS

CERT .....Computer Emergency Response Team

CIRT .....Computer Incident Response Team

CJCSI .....Chairman of the Joint Chiefs of Staff Instruction

CND .....Computer Network Defense

DAA.....Designated Approving Authority

DoD.....Department of Defense

DoDD.....Department of Defense Directive

DoDI .....Department of Defense Instruction

FISMA .....Federal Information Security Management Act

HA.....Health Affairs

HIPAA .....Health Insurance Portability and Accountability Act

IA .....Information Assurance

IAM.....Information Assurance Manager

IAO .....Information Assurance Officer

IS.....Information System

JMISO.....Joint Medical Information Systems Office

MHS.....Military Health System

PEO.....Program Executive Office

PHI.....Protected Health Information

SA .....System Administrator

SI.....Sensitive Information

TMA.....TRICARE Management Activity

TRO.....TRICARE Regional Offices

MHS Information Assurance
Computer Incident Reporting Form

Use this form to report incidents to the MHS Information Assurance Program Office. Send an electronic copy to the DAA and MHS IA Program Office, or fax it to (703) 681-8814.

Incident Number: _____ Category (defined below): 1 2 3 4 5 6 7 8

Date of Incident: _____ Time of Incident: _____

1. Reporting Organization Information:

Organization: _____

Name: _____

Section: _____

Telephone #: _____

E-mail Address: _____

2. Target Host Information:

Host IP: _____

Host Machine Name: _____

Classification Levels:

Classified _____ /Sensitive But Unclassified _____ /Non-Sensitive _____

System Mission: _____

Operating System: _____

3. Source(s) Information:

Source(s) IP: _____

Source Host Name: _____

Source Name and Address: _____

4. Intrusion Information:

Type of Incident or Attack: _____

How Detected: _____

Description of Incident: _____

Was System Compromised? Yes _____ No _____

Impact on Operation: _____

Countermeasure(s): _____

5. Notification:

Network Administrator: _____

Firewall Administrator: _____

LAN Administrator: _____

Network Security: _____

Virus Section: _____

Information Systems Security Officer: _____

Federal Computer Incident Response Team: _____

Law Enforcement Agency: _____

6. Additional Details (Please include here any information not detailed above):

_____

_____

_____

_____

_____

Incident Category Definitions:

Category #	Definition
1	Unauthorized Root / Administrative Access
2	Unauthorized User Access
3	Unauthorized Attempted Access
4	Denial of Service
5	Poor Security Practice
6	Unauthorized Probe / Information Gathering
7	Malicious Logic
8	Misuse